COMPUTER SYSTEMS SECURITY

CAT 1

GROUP D

BITC01/1500/2021 LIAN MWAURA
BCSC01/ 0039/2021 ZEPH ASEKA
BCSC01/0019/2021 JOHNSON KANYI
BITC01/0919/2021 JOSEPH KIMANI
BITC01/0905/2021 SHEILA BLESSINGS

Q1: Research on basic cryptography.

Cryptography is the study and practice of techniques of securing information and communication, ensuring that only authorized parties can access or understand it by converting it into another format.

Cryptographic techniques:

Encryption – the process of converting plaintext into ciphertext using a cryptographic algorithm and a key

Decryption – the reverse process of converting ciphertext back to plaintext; using the correct decryption key.

Cryptographic Keys: Keys are essential components used in encryption and decryption. They can be symmetric (same key for both encryption and decryption) or asymmetric (different keys for encryption and decryption).

Hashing: A one-way function that converts data into a fixed-size string (hash) which cannot be reverted to its original form.

Digital Signatures: Used for verifying the authenticity of messages or documents

Public Key Infrastructure (PKI): A system of digital certificates and Certificate Authorities (CAs) used for managing key distribution and identity verification.

Q1: Research on basic cryptography.

Application of cryptography:

- **Secure Communications**: Ensures that messages and data remain confidential between sender and recipient. Think of encrypted messaging apps like WhatsApp.
- **Data Protection**: Guards sensitive information in storage against unauthorized access, whether on your phone, cloud storage, or a corporate database.
- **Digital Signatures**: Verifies the authenticity and integrity of digital documents, ensuring they haven't been tampered with.
- **E-commerce**: Secures online transactions, keeping your credit card information safe when shopping on platforms like Amazon.
- **Network Security**: Shields data as it traverses networks, using protocols like SSL/TLS to secure websites and online services.

Q1: Research on basic cryptography.

- **Password Storage**: Uses cryptographic hashing to store passwords securely, so even if a database is breached, the actual passwords aren't exposed.
- **Blockchain**: Underpins cryptocurrencies like Bitcoin, ensuring secure and verifiable transactions on the blockchain.

Q2: Compare symmetric and asymmetric key cryptography

Aspect	Symmetric Key Cryptography	Asymmetric Key Cryptography
Keys Used	Uses one key for both encryption and decryption	Uses a pair of keys: one public and one private
Speed	Generally faster due to less computational overhead	Slower due to complex calculations involved
Key Management	Requires secure distribution of the secret key to all parties	Public key can be freely shared; only private key must be kept secure
Use Cases	Best for encrypting large volumes of data, e.g., AES for disk encryption	Ideal for digital signatures, SSL/TLS, and email encryption
Security Level	Highly secure if the key is kept secret but can be compromised if intercepted	More secure for initial connections as only the private key must remain confidential

Q3: Distinguish between the following: Cryptography, Cryptanalysis and Cryptology.

- **Cryptography**: The practice and study of designing algorithms and protocols to secure data, ensuring confidentiality, integrity and authentication.

- **Cryptanalysis**: process of analyzing and breaking cryptographic systems, with the intention of uncovering weaknesses.

- **Cryptology:** The broader field that encompasses both cryptography and cryptanalysis. It is the science of secure and private communication, covering all aspects of creating and analyzing secure communication methods.

Q4:CloudCo's Machines as Tor Entry and Exit Nodes: Why It's a Bad Idea

- **Overview of Tor Network**

The Tor network allows users to browse the internet anonymously by obscuring their IP addresses protecting user identity from tracking hence bringing about privacy and anonymity of users

Even though CloudCo's machines offer fast network speeds, low latency, and high bandwidth, using them as Tor entry and exit nodes can still pose significant risks:

- **Centralization of Power**: As we said Tor's strength lies in its decentralization, where nodes are scattered among volunteers worldwide, making it difficult for any one entity to monitor traffic. If CloudCo, a single organization, provides both entry and exit nodes, it introduces the risk of centralized surveillance. CloudCo could potentially monitor which users are entering and exiting the Tor network, compromising anonymity.

Q4:CloudCo's Machines as Tor Entry and Exit Nodes: Why It's a Bad Idea

- **Trust Issues**: While CloudCo may claim to be trustworthy and act in good faith, users cannot be certain of this. If CloudCo were to cooperate with authorities or get compromised, they could potentially reveal user data. Tor's security model assumes that no node can be trusted absolutely.

While leveraging CloudCo machines can enhance performance in the Tor network, risks associated with centralization, trust, and potential exploitation of vulnerabilities need careful consideration. This shift challenges the core principles of Tor's anonymity model.

Q5: Why Backtracker is Not Working Well for Ben

- A **Backtracker** is a tool that provides a valuable resource for web application security by helping track the origin of security intrusions by analyzing system logs and data dependencies.
- It is most effective when used in controlled environments where attacks can be isolated and logged. Here's why Ben's Backtracker setup is not working well:

1. **Concurrency Issues**: Ben is running Backtracker on a live system where many users are actively interacting with the web application. SQL injection attacks modify shared databases, and multiple users accessing the system at the same time can generate a large number of data dependencies. Backtracker may struggle to pinpoint the exact source of the attack due to overlapping user activities.

Q5: Why Backtracker is Not Working Well for Ben

2. Noise in the Data

Backtracker works by tracing changes in system files and processes. In a multi-user environment with active traffic, it will log numerous system changes unrelated to the attack, making it harder to trace the actual path of the malicious activity. The legitimate activities of other users may obscure the malicious action, resulting in inaccurate traces.

3. SQL Injection Complexity

SQL injection vulnerabilities exploit the application's interaction with the database. If Backtracker is not fine-tuned to handle web-based database attacks specifically, it might miss or incorrectly trace the source of SQL injection attacks. The tool is more effective for file-level changes and may not track sophisticated database-level changes as accurately.